京东云

备份和容灾技术白皮书

构建让客户安心的系统

2019-11-27

目录

1 京东云介绍

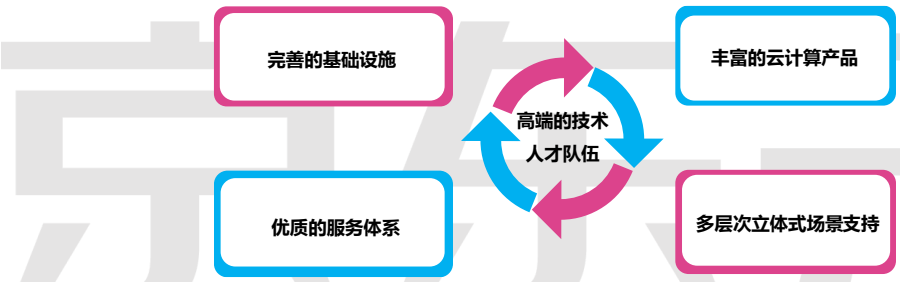
1.1 京东云概况

京东云(JD Cloud)是京东集团旗下的全平台云计算综合服务提供商，拥有全球领先的云计算技术和丰富的云计算解决方案经验。为用户提供从 IaaS、PaaS 到 SaaS 的全栈式服务(Full Stack)，从 IDC 业务、云计算业务到综合业务的全频道服务(Full Spectrum)，以及包含公有云、私有云、混合云、专有云在内的全场景服务(Full Services)和跨行业的全生态云服务(Full Ecosystem)。同时，京东云依托京东集团在云计算、大数据、物联网和移动互联网应用等多方面的长期业务实践和技术积淀，形成了从基础平台搭建、业务咨询规划，到业务平台建设及运营等全产业链的云生态格局，为用户提供一站式全方位的云计算解决方案。

当前京东云具有可信云服务认证、支付卡行业数据安全标准认证(PCI DSS)、ISO27001 信息安全管理体系国际认证、ISO9001 质量管理体系认证、信息系统等保三级安全认证、CSA STAR 云安全认证、CSTAR 云计算安全评估认证等数十项资质认证。

1.2 京东云主要优势

京东云经过多年的发展，在不断的技术积累与创新下，形成了如下五大优势：



高端的技术人才队伍

京东云基于京东集团近 20 年的互联网技术积累，组建了一支成熟稳定的以高端技术人才为核心主力的人才队伍。在一批云计算行业领军人物的带领下，京东云技术人才队伍不断拼搏创新，实现业界领先的技术实力和服务能力。

完善的基础设施

京东云在覆盖全国的 4 个地域建设了多个设施先进、功能完善的 IDC。地域

之间通过超高带宽的骨干网络连接，形成巨大的网络数据传输优势。基于稳定可靠的基础设施，京东云以一流的技术和运维能力向用户提供安全、专业、稳定、便捷的云计算服务。

丰富的云计算产品

经过多年的努力，基于京东云对整个行业的深入理解，当前公有云已经为全社会贡献出种类繁多的产品和服务。京东云通过人工智能、大数据和物联网等行业领先的高技术产品，为用户业务的快速发展助力赋能。

多层次立体式场景支持

京东云通过功能丰富的标准产品提供 IaaS、PaaS、SaaS 等全栈式云计算服务，能够很好的支持公有云、私有云、混合云、专有云等多种场景，能够对外提供 IDC 业务、云计算业务、综合业务等全频段业务服务，还能够针对用户需求提供快速的定制化开发，充分满足用户对云计算的全方位需求。

优质的服务体系

京东云基于用户服务和通用技术服务等基础服务，以促进用户成功为理念，建立了金牌服务、优质架构服务、应急服务、迁移服务、系统优化服务等高技术价值服务，形成了基础稳固、技术先进、用户满意的层次化服务体系，客户服务更加专注、贴心，技术保障更加有力。

2 技术概述

当前，IT 信息系统已经渗透到各行各业的业务建设之中。用户业务系统的稳定可靠运行是用户业务发展的重要基础。京东云通过不断技术积累，并且通过搭建可靠的基础设施平台，为用户提供数据备份和系统容灾技术保障，成为行业中最值得信赖的云计算厂商。

2.1 备份和容灾技术发展概况

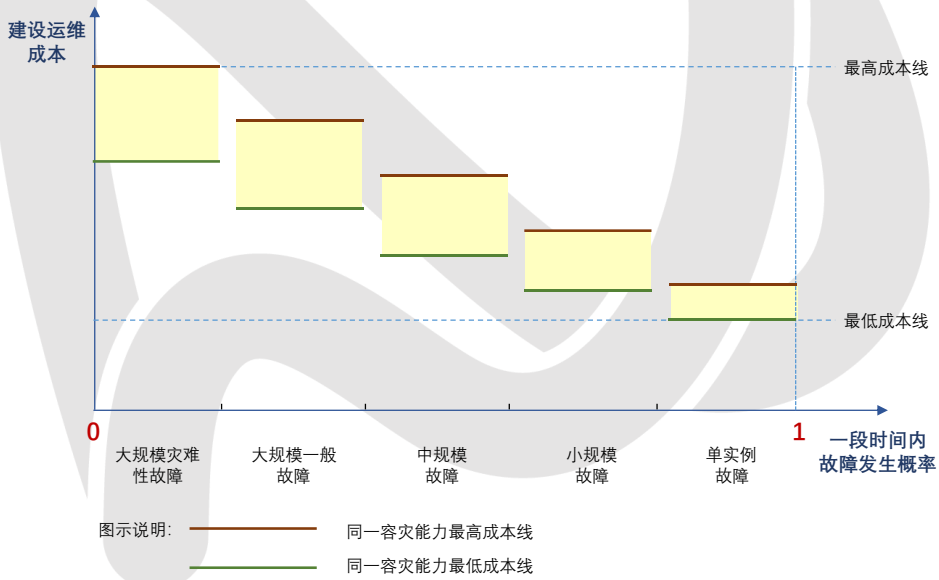
备份和容灾技术起源于人类的技术发展，在各种工程、系统建设过程中都有广泛应用。中国古代著名水利工程都江堰通过分水鱼嘴和宝瓶口等结构的联合运用，实现了抗洪容灾的功能。

由于 IT 信息系统在不受保护的情况下非常脆弱，比如断电即刻导致系统瘫痪，故 IT 信息系统是备份和容灾技术的重要应用领域。对于政府、组织和企业用户，一旦重要 IT 信息系统停摆，业务体系将受到巨大冲击。据 University of Minnesota 的研究，当发生重大数据丢失事故后，半数以上的公司会在两三年内

倒闭。因此，IT 信息系统的备份和容灾技术应用，越来越重要，也越来越被重视，国家和行业标准中规定了明确的技术要求。

备份和容灾在 IT 信息系统中主要指数据备份和系统容灾两项技术。数据备份技术是系统容灾技术的重要支撑，但数据备份技术也可以单独在系统中实施。最早在数据备份和系统容灾技术上有重大突破的是美国。早在 40 年前 SunGard 公司就在美国的费城建成了数据备份和系统容灾中心，用于保护金融业务系统。

当今，京东云紧跟数据备份和系统容灾技术发展的前沿，将既符合中国国情又遵循业界实践经验的完整数据备份和系统容灾解决方案贡献给用户。京东云重视每一个用户的业务长期稳定发展，将通过易用的工具、成熟的方案和可靠的服务提供最符合用户期望和利益的业务连续性保护。



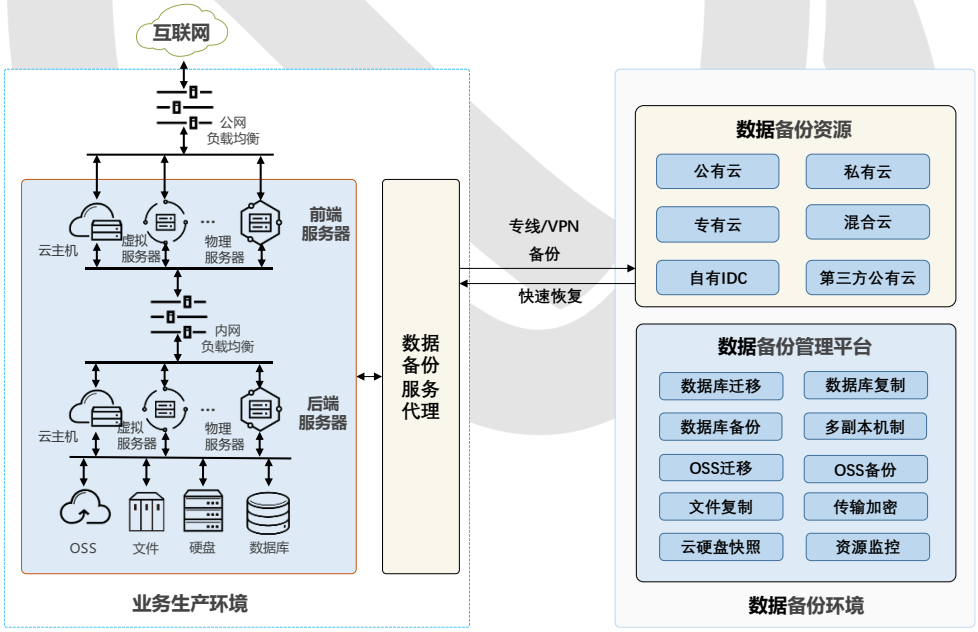
系统故障原因主要有外部因素和内部因素，根据不同的类型可以分为异常事件、事故事件和灾难事件等三个级别。异常事件是导致系统按照偏离设计的模式运行的系统内部原因，通常会在某些条件下触发并导致系统出现问题。事故事件是导致系统出现较严重问题的内部或外部原因。灾难事件是超出系统建设和维护人员控制能力并导致系统出现大范围严重问题的外部原因。基于业界的长期经验积累，通常异常事件、事故事件和灾难事件发生的概率逐级减小，但造成的损失和需要防止其造成持续损失所需要投入的成本逐级增大。

如上图所示，根据京东云多年的项目建设和维护经验，故障原因的类型、事件发生的概率和系统保护所需建设和维护成本的关系为一个分段图。为了保护系统最基本的可靠运行，需要投入不低于最低成本线的成本。为了实现更好的系统保护，需要投入更高的成本。每提升一个系统的保护级别，都会产生成本的跃升。在能够抵抗同等规模故障的系统中，根据技术选型的不同会产生不同的建设和运维成本，不同的技术方案也同时对系统的稳定性、安全性和性能等关键指标要素产生影响。

2.2 京东云数据备份技术

数据备份技术的核心是将生产环境中的在线数据通过技术方法备份到离线环境。当系统发生问题，则技术人员能够基于备份数据将数据恢复到理想的状态。备份数据并不用于业务生产，但保留关键版本的备份数据对业务系统的长期有效运行具有非常重要的意义。

京东云在向用户提供丰富的云资源产品的同时，深刻总结数据备份领域的技术经验，对用户开放技术能力，并进行数据备份技术赋能。根据业务场景和备份环境的不同，京东云提供两种主要的数据备份方式：一是支持在云平台上建立数据备份环境并将用户的业务系统核心数据安全可靠地备份到云平台上。二是支持将数据通过网络专线或 VPN 的方式备份到用户自有的数据中心。



京东云支持京东云平台或用户自建数据中心的数据库、文件、对象存储备份。通过网络专线或 VPN 在用户的业务生产环境和数据备份环境之间搭建安全可靠的网络数据传输通道。若用户的业务生产环境和数据备份环境都搭建在京东云公有云上，则能够在业务生产环境和数据备份环境之间搭建高带宽网络通道，实现数据安全高速传输。京东云通过部署数据备份服务或数据备份工具，使数据备份过程简单高效。并提供强大的资源监控工具，当系统出现问题，技术人员能够及时准确了解情况，并进行快速稳妥处理。

在平台支持方面，京东云支持用户将数据备份到京东云公有云、私有云、专有云和混合云平台上。还支持用户将数据备份到用户自有 IDC 中或第三方公有云上，为用户带来极大方便，提供让用户满意的数据备份解决方案。

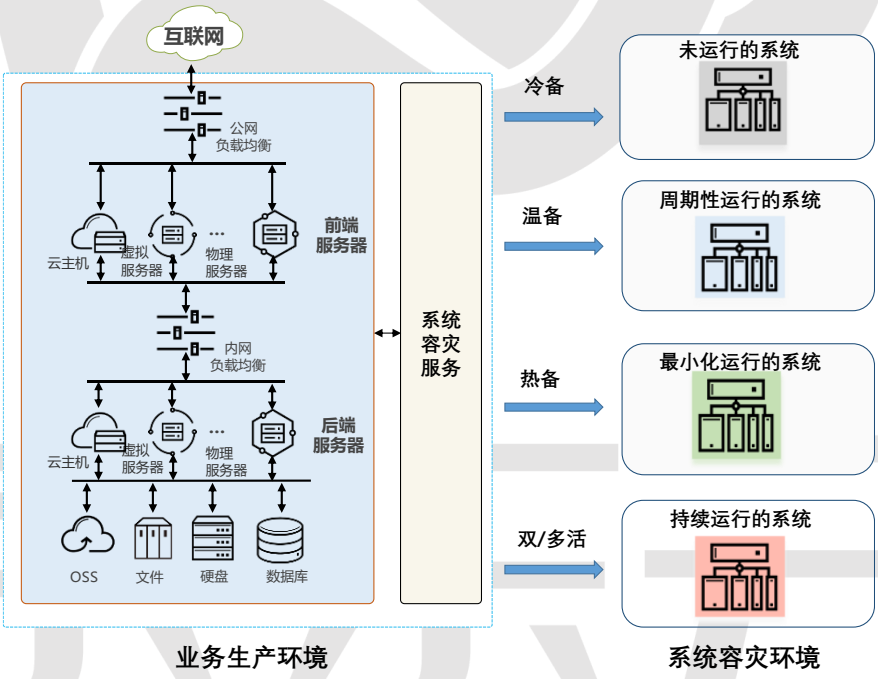
在数据备份技术方面，京东云支持数据库的迁移和复制、对象存储中数据的迁移和复制、文件系统中的文件迁移，并支持数据传输加密保护。利用云平台提

供的快照功能，用户能够快速将数据恢复到所需的版本。京东云也提供完善的资源监控系统，使用户能够完全掌握数据备份过程中系统的运行情况，并在发生异常时发出报警提示。

2.3 京东云系统容灾技术

系统容灾技术的核心是当信息系统遭遇灾难并导致严重故障时能够保护客户数据安全和保持关键核心业务稳定。能够造成系统严重故障的灾难一般有地震、水灾、火灾、军事袭击、不当市政施工等，这些灾难在社会运行过程中均有一定发生的概率，因此在关键系统设计和建设时采取系统容灾技术进行有效保护非常重要。

京东云支持对系统的数据级容灾和应用级容灾。数据级容灾支持对客户的数据进行备份、同步复制或异步复制，维护客户数据安全，确保严重故障发生时关键数据可用和可恢复。应用级容灾支持建立与业务生产环境相匹配的备份系统，保证故障发生时及时将业务流量切换到备份环境，使业务系统持续对外提供服务。

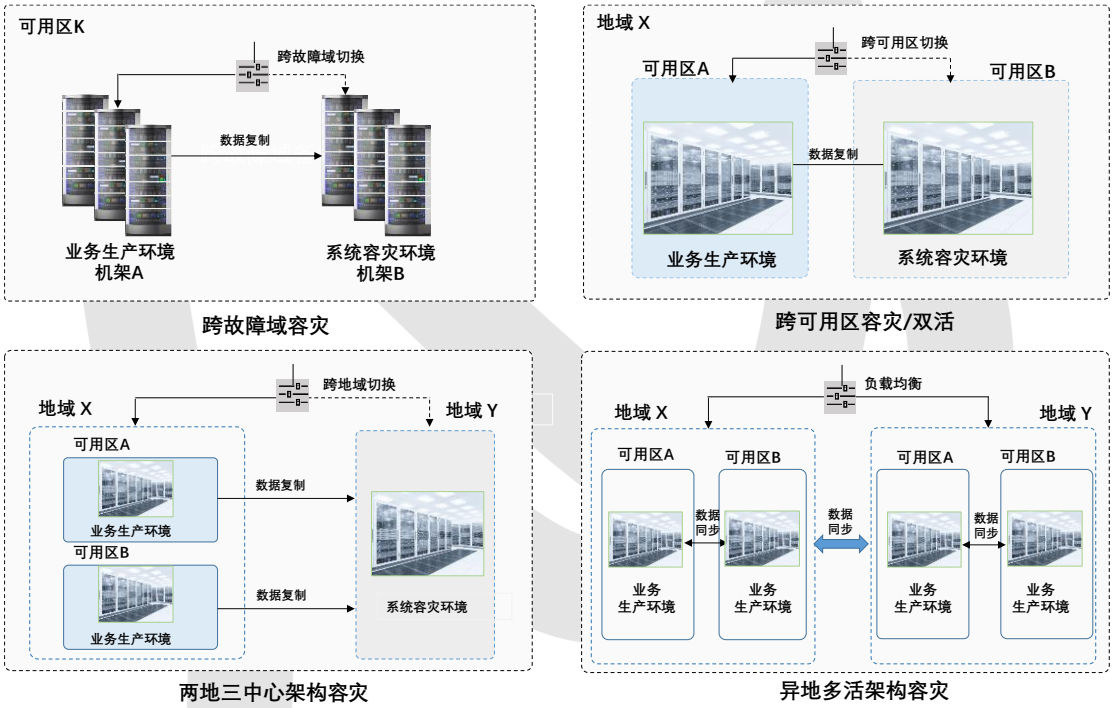


京东云能够根据客户系统容灾需求并基于系统架构制定有效的容灾方案。通过丰富多样的系统容灾方案支持，提供多种系统容灾能力，满足客户的系统容灾需求。

- **冷备**：支持数据的定期备份，并利用未运行的系统作为生产系统的备份环境，当大范围系统故障发生时启动备份系统支撑业务系统运行。
- **温备**：支持数据的定期备份或周期性同步，利用周期性运行的系统作为生

产系统的备份环境，备份环境中的系统定期开启并进行必要的系统同步操作。

- **热备**：支持数据的定期备份或数据复制，在容灾环境建立最小化运行的热备份系统，当大范围系统故障发生时容灾环境接替原生产环境提供服务，并根据业务情况扩展资源。
- **双/多活**：支持数据的同步复制，建立两个或多个相互隔离的业务生产环境，并保持各个业务生产环境的数据一致性。



利用京东云底层资源的容灾能力，支持多种系统容灾架构，充分满足不同行业客户的实际业务需求。

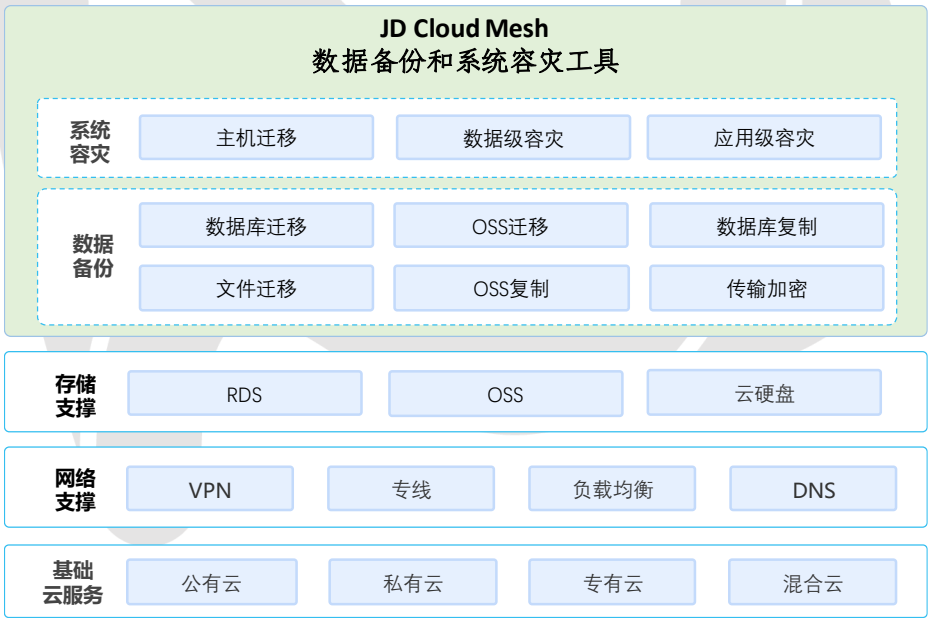
- **跨故障域容灾**：京东云提供故障域支持，实现了在同一可用区内相互独立的供电、网络设施等基础设施建设。
- **跨可用区容灾/双活**：利用京东云的负载均衡技术，客户能够便捷地实现跨可用区系统容灾，或实现两个可用区内双活系统架构。京东云在同一地域内的可用区之间相隔数十千米，采用相互独立的双路供电系统，能够满足大多数客户的容灾架构需求。
- **两地三中心架构容灾**：通过在不同的地域搭建业务系统，使系统获得极大的抗灾能力。
- **异地多活架构容灾**：在多个可用区和多个地域建立同时运行的业务生产系统，在提升系统大范围抗灾能力的同时，能够保障系统最佳的灾后恢复速度。

不同的容灾系统架构对应不同的系统容灾能力和灾难发生后的系统恢复效

率，同时也会产生不同的系统建设和维护成本。京东云支持客户根据行业标准和实际需求选择最适合的容灾架构。

2.4 平台工具和服务

京东云提供专业的 JD Cloud Mesh 数据备份和系统容灾工具集，如下图所示，全面支持客户快速便捷实现数据备份和系统容灾。支持数据库迁移、OSS（对象存储）迁移、文件迁移，同时支持 OSS 复制和数据库复制。支持传输加密功能，为数据传输提供可靠的安全保障。支持主机迁移、数据级容灾、应用级容灾，能够全面提升客户系统的抗灾能力，并实现快速的灾后恢复。支持对业务系统和容灾系统进行全方位的资源可视化监控，能够及时发现故障并进行有效的预警。



在 JD Cloud Mesh 基础之上，京东云为客户提供多层次平台服务，主要包括备份和容灾系统建设和运维中的基础云服务、网络支撑、存储支撑。

基础云服务。京东云根据安全性、数据规模、资源扩展性等客户需求，提供公有云、私有云、专有云、混合云等多种可选的备份容灾环境，通过专业的技术服务帮助客户高效合理的构建云计算环境下的业务系统和备份容灾系统，并提供可靠的后期技术保障支持。

网络支撑。京东云通过支持 VPN、网络专线、负载均衡、DNS 等多种网络技术，帮助客户在建设备份和容灾系统时获得可靠的网络技术保障，确保数据传输的安全和灾后数据流量切换的及时有效。

存储支撑。京东云通过支持多种 RDS（关系型云数据库服务）、海量对象存储 OSS 和大容量高性能云硬盘，为客户提供可靠的数据备份环境，并基于多副本机制确保客户数据不会丢失。

2.5 安全保障

京东云在实现数据备份功能的同时，还通过有效的技术手段确保备份过程和恢复过程安全可靠。

京东云遵循业界先进的安全标准保障客户系统和数据全生命周期安全，采取平台安全保护措施、安全管理和信息安全技术等手段进行全面安全体系建设。京东云通过了中国信息通信研究院可信云服务认证，标志着京东云成为国家认可的安全、可信的云服务商。还通过了公安部信息系统安全三级等保认证，标志着京东云符合国家在信息系统安全方面的技术和管理要求，能够应对信息安全威胁。同时京东云还通过了数十项资质认证，充分保障云平台和客户数据的安全。

云平台安全保障方面，具有 T3 级的数据中心，提供高水平的系统运维，确保硬件设备、云平台虚拟化层、系统监控的安全可靠。

数据安全方面，系统通过网络安全、数据安全和数据可靠性保障等措施确保数据备份过程的安全。在网络传输过程中，支持建设网络专线保障数据安全快速传输，也支持搭建 VPN 实现数据加密传输，并通过 SSL 数字证书进行身份认证，有效保护数据在网络传输过程中的安全。在数据安全保护方面，利用有效的身份认证和访问控制机制，确保只有合法客户才能访问在权限范围内的数据。利用静态数据加密技术，保护在数据备份端落地存储的数据，满足在公有云等开放环境中也能确保客户数据安全。利用云平台提供的组合隔离技术，防止数据被非法访问。在数据的可靠性保障方面，支持数据库和对象存储的数据复制和多副本机制，并通过数据的完整性和一致性校验确保数据不会丢失。

在系统可用性保障方面，支持云主机热迁移、高可用组、跨可用区高可用、跨地域高可用，全面保障系统的长期稳定运行。

3 数据备份解决方案

3.1 适用场景

我国信息技术发展迅猛，IT 信息系统的应用领域极为广泛。但从各行业和部门信息系统建设和维护状况中，可发现仍然存在下面的诸多问题需要解决：

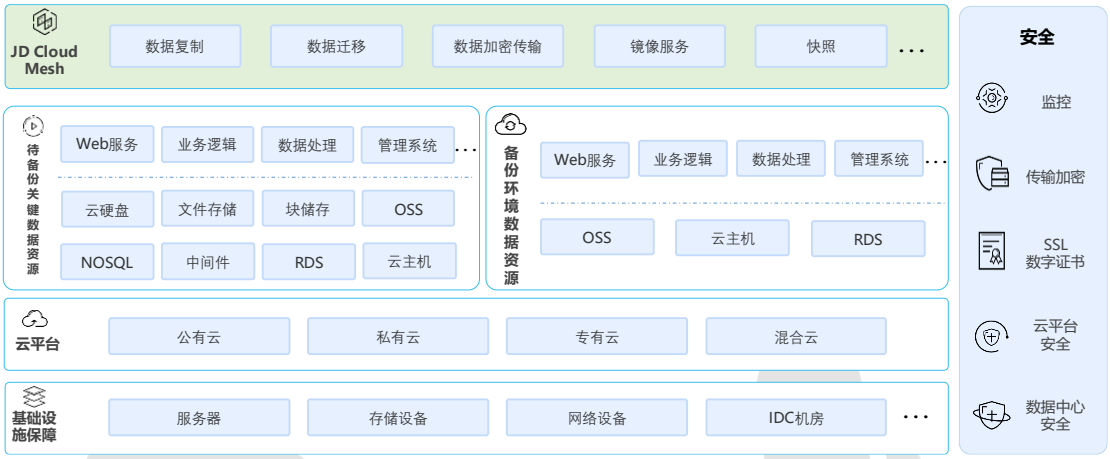
- 在互联网、游戏、传媒等行业，要不断根据新需求对系统进行快速迭代，会发生更新导致数据污染、数据损坏等异常。
- 由于产业发展迅猛，导致技术人才缺口增大，出现系统运维人员技术能力参差不齐的情况，易出现系统运维操作给系统数据带来负面影响的情况。
- 存储介质存在固有的故障率，在系统集群规模较大的情况下，发生存储硬件故障的概率较大，给系统中存储的数据带来丢失或不一致的风险。

京东云非常重视对数据的可靠性和一致性进行保护，为提升客数据的安全性，京东云提供的数据备份解决方案除能够较好地解决上述的几个主要问题，并能够适用于以下一些主要场景：

- 数据为核心资产之一。对某些客户，数据是核心资产，若失去数据则可能导致客户失去在市场中的竞争优势或失去业务运行的基础。京东云能够提供成熟的数据备份技术，并提供安全可靠的数据备份环境，帮助客户保护数据，维护客户核心利益。
- 标准、规范要求。数据备份已成为国家和行业针对重要业务系统提出的标准和规范的重要组成部分。京东云能够帮助客户实现满足标准和规范要求的 IT 支撑系统，使客户的业务系统满足监管机构的技术要求。
- 数据影响业务发展。在政府、组织、企业中，数据对其未来的发展起到越来越重要的作用。京东云能够帮助政府、组织、企业等重要客户实现可靠的数据备份系统，支撑系统快速迭代发展，保障数据的可靠性和一致性。
- 旧系统升级改造。由于技术发展历史原因，某些较老的信息系统的数据可能还存储在没有有效保障的环境，客户不希望投入过多经费对系统进行升级。京东云能够为客户提供高性价比的数据备份解决方案，利用京东云丰富的 IaaS 资源，帮助客户快速而又低成本地实现原有系统的改造，保障数据的安全。

3.2 技术架构

依托于京东云提供的丰富和先进的 IT 资源，基于京东云 T3+级的数据中心建设能力，京东云数据备份技术架构如下图所示。

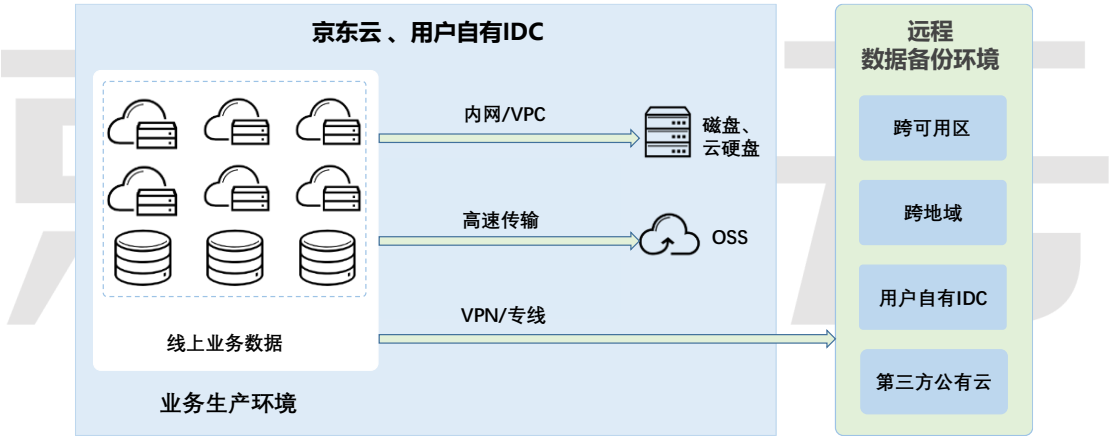


京东云通过完善的数据中心建设，为客户的数据备份提供可靠的基础设施保障。在京东云数据中心内的服务器、存储设备和网络设备等硬件资源都有业界技术领先的运维人员负责维护，确保服务器集群和基础网络的稳定运行。为支持客户数据备份业务，京东云提供公有云、私有云、专有云、混合云等多种云平台，按照客户的个性化需求设计最合理的数据备份方案。在京东云的云平台上，支持非常丰富的云平台资源，用于承载客户的业务系统和数据备份系统，提供具有高性价比的 IT 资源。通过专业的京东云 JD Cloud Mesh 平台，提供数据备份平台工具，帮助客户的业务系统快速实现数据复制、迁移、加密传输等多种数据备份所需的功能。

3.3 技术方案

京东云为客户提供网络架构，数据备份与恢复和主要指标三种技术方案。

3.3.1 网络架构



- 线上业务数据备份到云硬盘或硬盘

在京东云或客户自有 IDC 内，支持将客户的线上业务数据通过京东云 VPC 或客户内网备份到京东云云硬盘或客户硬盘中。京东云 VPC 支持 IP 地址网段

划分，并通过支持安全组和自定义路由策略，实现安全隔离的客户专有网络。利用京东云提供的 VPC 构建安全、稳定、易扩展的局域网络，满足客户进行快速数据备份的需求。并利用云硬盘多副本机制，确保客户数据不会丢失。

- 线上业务数据备份到 OSS

OSS 是京东云自主研发的大规模分布式对象存储服务，面向企业和个人客户提供高可用、低成本、高安全性的云端存储服务。OSS 支持通过京东云 VPC 内网访问，网络数据流量免费，可实现备份数据高速传输。同时，OSS 提供标准存储、低频存储、归档存储、低冗余存储等 4 种存储方式，利用低频存储或归档存储等两种存储方式实现数据备份能够大幅降低客户的数据存储成本。

- 线上业务数据备份到远程数据备份环境

在远程数据备份的场景下，为了确保数据传输安全，京东云支持客户通过 VPN 或网络专线将待备份数据传输到数据备份环境中。基于客户的业务需求，京东云支持跨可用区数据备份、跨地域数据备份、客户自有 IDC 数据备份和第三方云平台数据备份等多种远程数据备份方式。

可用区（Availability Zone 或 AZ）是电力及网络之间互相独立的物理区域，京东云在同一地域内可支持多个内网互通的可用区，实现较好的故障隔离。利用跨可用区进行数据备份能够使系统抵抗数据中心范围（数十千米）的灾难，并且具有非常高的网络传输带宽。

京东云的互联网机房分布在全球多个位置，这些位置称为地域（Region）。每个地域都是一个独立的地理区域，在供电、供水、网络等基础设施层面每个地域都完全独立，不同地域之间相隔数百至数千千米。采用跨地域进行云数据备份能够使客户的业务系统抵抗地震、海啸等巨大规模自然灾害导致的区域性系统故障。

京东云支持客户将数据安全地备份到客户自建的数据中心，也支持将数据备份到第三方云平台，帮助客户根据自身业务特点自由选择相应备份方式。

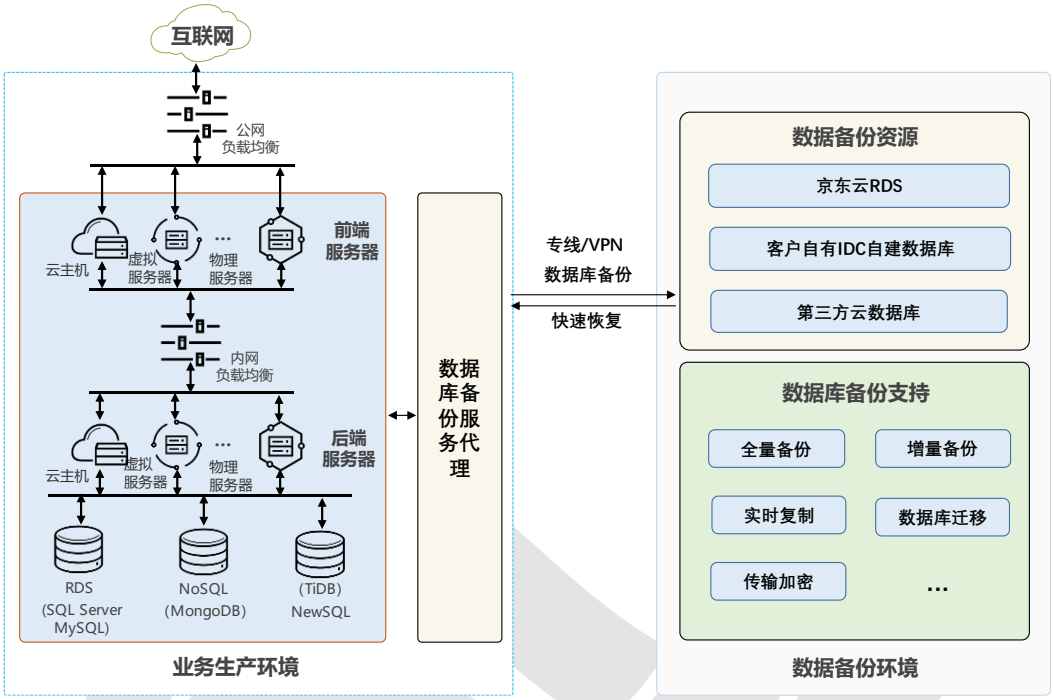
3.3.2 产品数据备份与恢复

京东云的数据库及存储产品在 JD Cloud Mesh 的数据备份工具的帮助下支持将客户线上业务数据通过网络专线或 VPN 进行备份。当系统遇到自然灾害或人为灾难导致大范围故障时，京东云提供及时、专业的技术支持服务，帮助客户快速恢复关键数据，降低系统损失。

3.3.2.1 数据库

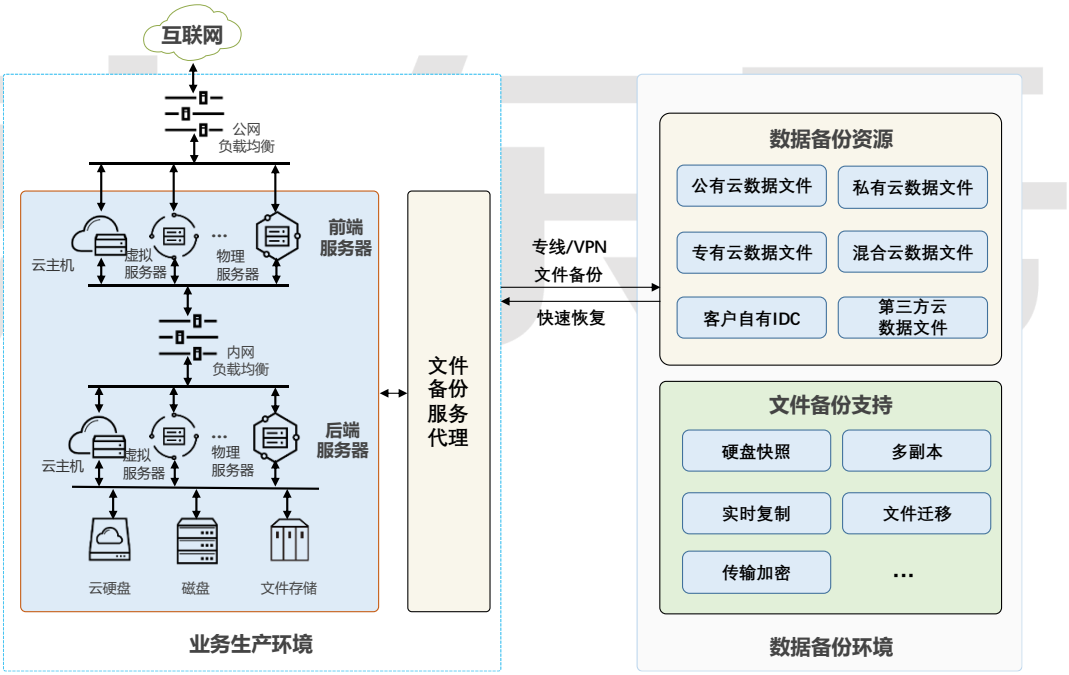
京东云云硬盘本身具有主从高可用架构，能够保障很高的数据可用性和可靠性，同时支持备份数据同步至京东云存储，支持 3 副本存储，确保京东云 RDS 数据安全。京东云数据库备份工具和服务支持 MySQL、SQL Server 等关

系型数据库，支持 MongoDB 等非关系型数据库，也支持 TiDB 等 NewSQL 数据库。京东云通过数据库备份服务代理，将待备份的数据通过网络专线或 VPN 备份到京东云的 RDS、客户自建数据库和第三方云数据库。



京东云提供全量备份、增量备份、实时复制、数据库迁移等数据库备份服务，满足客户不同的数据安全性需求。当灾难发生并导致业务系统数据损坏时，备份环境中保存的数据确保客户关键业务数据不丢失，同时京东云将提供及时的技术支持服务，帮助客户快速恢复业务生产数据。

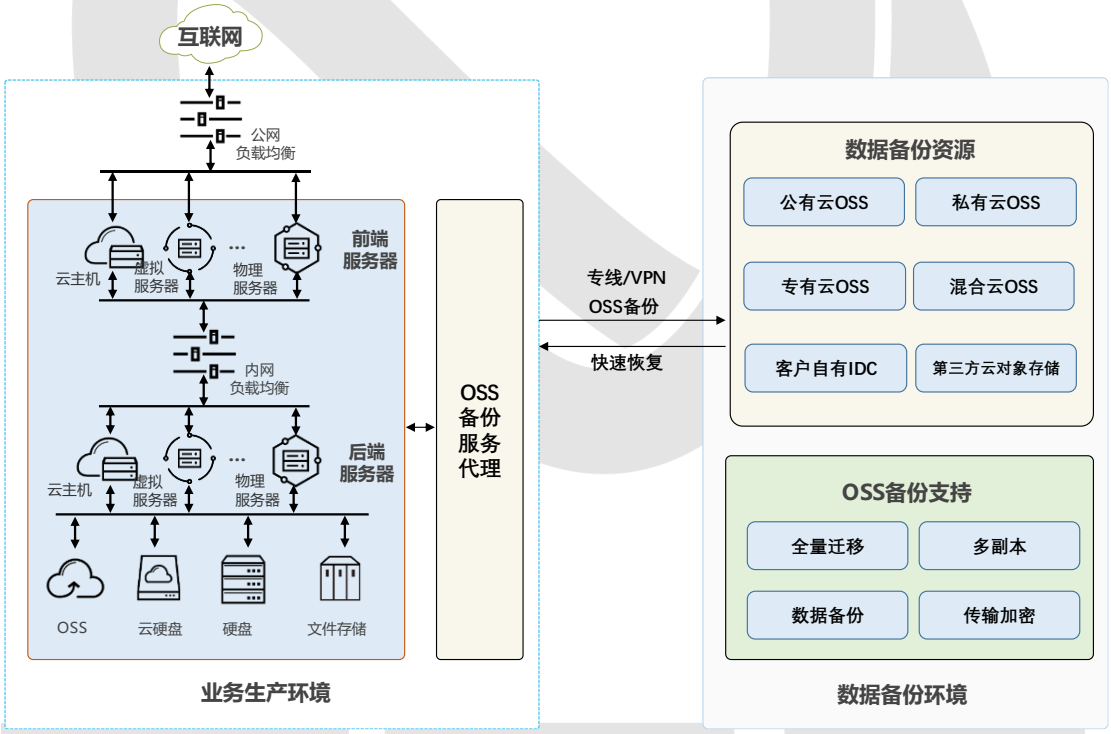
3.3.2.2 块存储和文件



京东云云硬盘和云文件服务产品支持多副本机制，能够保障极高的数据可靠性。同时京东云支持通过备份服务代理将待备份的数据通过网络专线或 VPN 备份到数据备份资源平台。数据备份资源平台支持京东云公有云、私有云、专有云、混合云，也支持客户自有 IDC 或第三方云平台，从而满足不同客户的业务需求。

京东云提供硬盘快照、数据多副本、数据实时复制、文件迁移等备份方式。当灾难发生并导致业务系统数据损坏时，备份环境中保存的文件确保客户关键数据不丢失，同时京东云将及时提供服务支持客户快速恢复关键数据。

3.3.2.3 对象存储 OSS



京东云对象存储产品 OSS 本身支持多副本机制，能够保障极高的数据可靠性。同时，京东云支持将客户存储在对象存储、文件存储、云硬盘或硬盘中的数据，通过备份服务代理，将文件备份到京东云的公有云、私有云、专有云、混合云的 OSS 中，也支持将文件备份到客户自有 IDC 或第三方云平台的对象存储中。

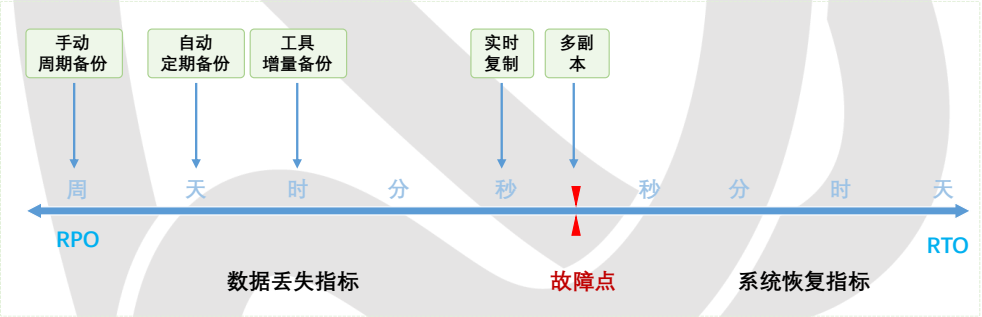
京东云提供 OSS 多副本机制、数据全量迁移、数据备份等备份方式。当灾难发生并导致业务系统数据损坏时，备份环境中保存的文件确保客户关键数据不丢失，同时京东云将及时提供服务支持客户快速恢复关键业务数据。

3.3.3 主要指标

京东云数据库与存储产品进行数据备份的主要指标如下表所示：

备份类型	支持的备份方案	主要指标
数据库备份	公有云 RDS 备份配置	RPO < 24 小时
	JD Cloud Mesh 备份工具增量备份	可配置，可实现 RPO < 1 小时
	JD Cloud Mesh 备份工具数据实时复制	RPO ≈ 0
块存储和文件备份	云硬盘快照（手动执行）	依赖手动执行频率，每天执行可实现 RPO < 24 小时
	JD Cloud Mesh 备份工具数据实时复制	RPO ≈ 0
对象存储备份	多副本机制	支持 99.999999999%数据可靠性
	JD Cloud Mesh 备份工具全量迁移	依赖手动执行频率
	JD Cloud Mesh 备份工具数据备份	可实现 RPO < 1 小时

利用多种技术手段，京东云支持如下图所示的数据恢复能力：



4 系统容灾解决方案

4.1 适用场景

IT 信息系统已经成为政府、各种组织和企业业务发展的关键，保障信息系统的稳定运行极为重要，但并非所有的系统都能满足长期稳定有效运行的要求。当系统没有依据客观情况进行合理的容灾设计的时候，会出现以下一些主要问题：

- 当系统容灾的设计缺少或不规范时，一方面会导致系统不符合国家或行业的规范，另一方面当系统遭遇故障或灾难时会对业务带来巨大安全风险，轻则造成业务的停顿，重则造成企业的消亡。
- 当容灾设计与实际需求不匹配时，由于大量的资源投入和人员投入，会产生额外的巨大开销，造成资源和人力浪费。
- 设计不合理的系统容灾系统也可能造成在发生事故或灾难时无法按预定的计划实现系统的恢复，对业务造成重大的冲击。
- 某些 IT 信息系统会承载多个客户的业务，不合理的容灾方案很可能在系统遭遇故障或灾难时对系统上承载的业务造成损害，严重时产生法律纠纷。

京东云基于系统容灾技术的深刻积淀，将系统容灾技术与国家、行业的规范以及客户的具体需求进行全方位的适配，提供性价比高且设计合规、合理的系统容灾解决方案，其适用的主要场景有：

- 符合国家或行业标准、规范要求。针对政府、金融等多个行业对系统容灾的要求，京东云提供符合标准和规范的系统容灾解决方案，使系统建设和运维符合监管要求。
- 符合客户的实际需求。针对客户的业务和系统需求，结合京东云的系统容灾实践，提供能够支撑客户业务长久发展的系统容灾方案，帮助客户降低建设和运维成本。
- 提供长期专业的技术支持。在客户系统运维人力不足的情况下提供长期的系统技术支持，通过定期的故障演练，增强客户系统的抗灾和恢复能力。

4.2 技术架构

京东云为客户提供系统容灾架构设计、数据级容灾方案、应用级容灾方案及安全保障等全方位的系统容灾技术支持，帮助客户轻松的实现符合业界规范和业务需求的容灾系统。

基于京东云的公有云、专有云、私有云和混合云等多种云平台的支持，实现客户业务系统的跨故障域、跨可用区容灾，还能实现更高级的两地三中心和异地多活等大型系统容灾方案。

数据级容灾方面，支持数据库和对象存储的定时备份和实时复制，支持文件的定时备份和手动备份，实现满足客户需求的 RPO 指标。

应用级容灾方面，通过主机迁移、系统复制和软件复制，实现业务系统的冗余保护，并通过支持冷备、温备、热备和双/多活技术，实现多种应用容灾。

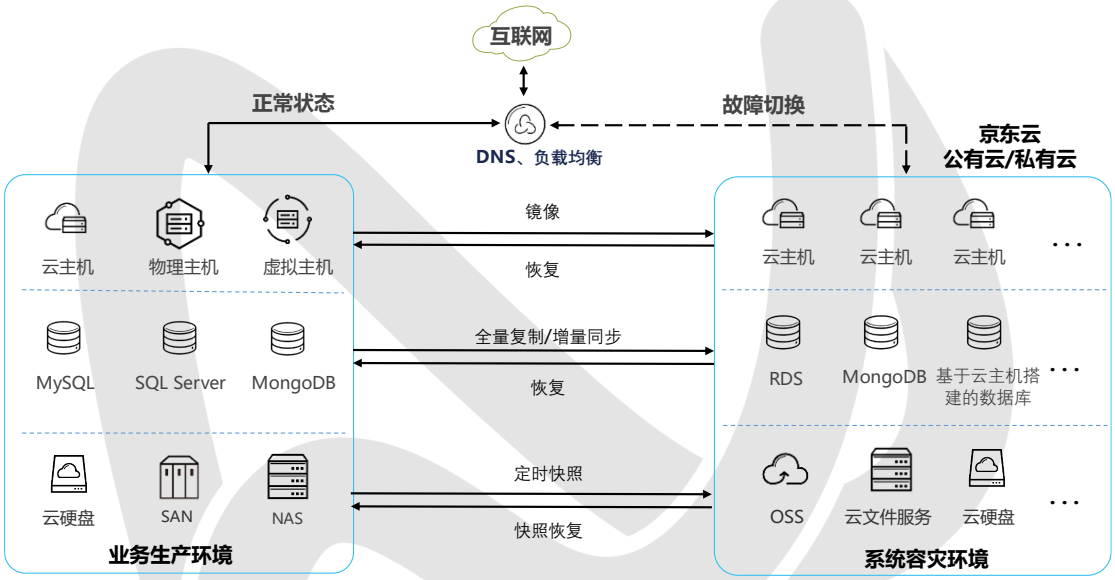
在安全保障方面，京东云利用功能完善、覆盖全面的监控系统能够实现快速的系统故障发现和预警，还能通过网络专线、加密传输保护数据传输的安全，并利用 SSL 数字证书机制确保只有合法用户能够访问关键系统和数据，从而从多个方面确保系统容灾的安全可靠。

4.3 技术方案

京东云利用云平台技术优势，支持多种系统容灾方案，提供公有云和私有云等不同容灾平台支持，并基于客户的具体需求支持数据级容灾和应用级容灾。

4.3.1 网络架构

京东云的系统容灾网络架构如下图所示：



京东云支持客户将业务生产环境备份到京东云公有云或敏捷专有云。

- 利用公有云云平台进行系统容灾。依托京东云公有云的海量主机和存储资源，能够帮助客户在进行系统容灾建设时和运维时大幅降低资源和管理成本。通过网络隔离和数据隔离技术实现系统容灾环境的租户隔离，确保客户在公有云系统容灾环境下的安全。
- 利用私有云云平台进行系统容灾。京东云私有云能保障客户系统安全性和数据隐私性，并提供定制化的系统容灾解决方案，可在业务系统大规模故障时支撑业务正常运行。支持为客户实现定制化容灾服务，包括专属的计算资源、存储资源、网络资源、操作系统、数据库、中间件、应用系统等 IT 资源，保障客户 IT 系统环境的独立性，完整性及稳定性。

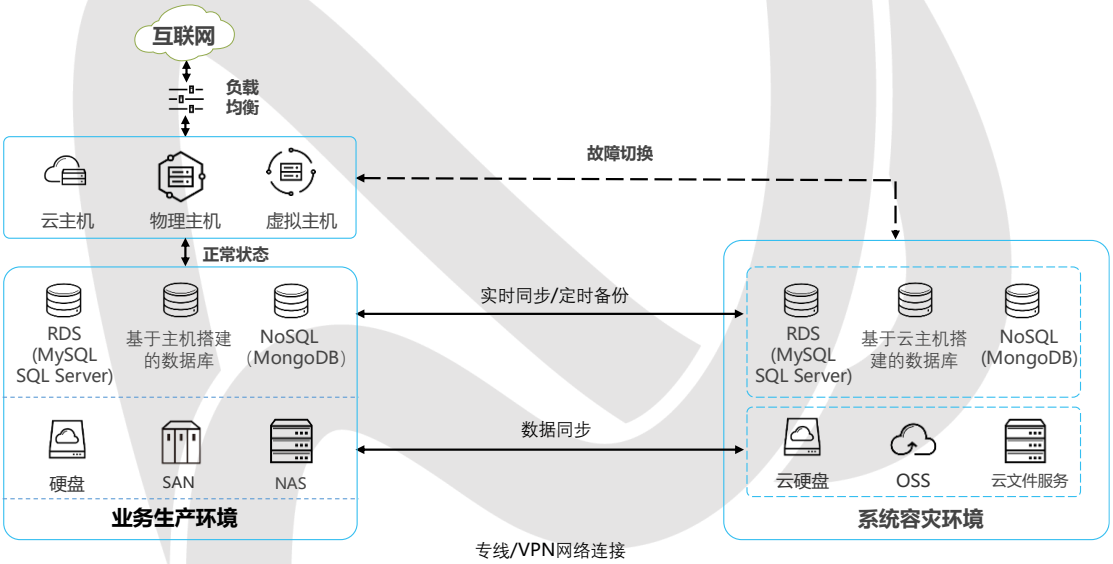
在数据级容灾方面，利用高速链路复制生产数据库（MySQL、SQL Server、MongoDB 等）的全量数据，并利用日志同步增量数据，可以在数据备份的同时，尽可能降低对生产环境性能的影响。对于存储系统中的文件，采用多副本、快照、实时复制等方式实现数据的容灾备份。

在应用级容灾方面，京东云支持同城双活、两地三中心、异地多活等高级系统容灾架构，支持在热备方案中进行云主机状态的快速同步，也支持利用镜像将数据中心的云主机、物理机备份到云平台。

利用先进的监控技术对业务生产环境进行实时监控预警，当灾难发生并导致业务生产环境的大规模故障时，监控系统能够及时发现故障并进行报警，管理员可以进行及时处理并将业务流量切换到系统容灾环境，保障业务正常运行。当生产环境恢复后，京东云支持将数据、生产日志及缓存等恢复到生产环境中。

4.3.2 数据级容灾

京东云通过支持系统的数据级容灾实现低成本的容灾系统，既能确保系统关键数据不会丢失还能大幅度降低容灾系统的建设、运维经费开销。

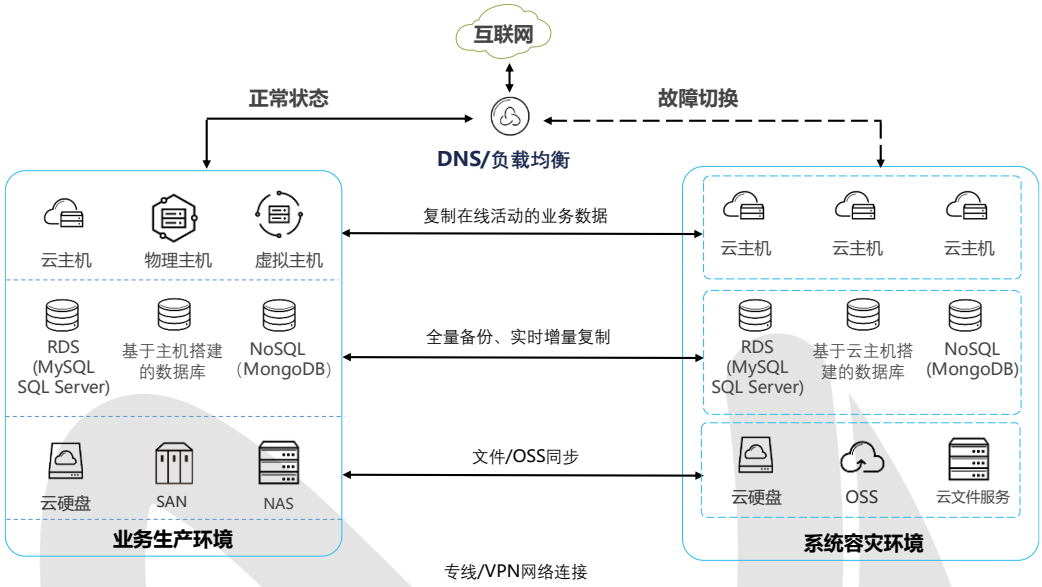


在业务生产环境正常的情况下，系统主机中的应用系统访问业务生产环境中的数据库、块存储、对象存储等数据。同时，系统中的所有数据都同步或异步复制到系统容灾环境中。京东云通过提供稳定可靠、成本较低的数据库和存储资源，搭建理想的系统容灾环境。一旦在业务生产环境中的数据库、块存储设备、网络文件存储系统、对象存储系统等发生严重的故障而导致数据不可用时，支持将应用系统访问的数据地址切换到系统容灾环境，确保数据的一致和系统的稳定连续运行。

数据级容灾相比于下述的应用级容灾能够节省部署冗余的计算环境，因此可以大幅度降低整体系统的建设成本。

4.3.3 应用级容灾

京东云应用级容灾技术能够帮助客户实现更优化的系统容灾支持，确保某个范围发生重大灾难时客户的业务系统依然能够正常运行并对外提供可靠的服务。



建设应用级容灾系统时，需要在相隔一定距离的至少两个数据中心同时建设应用系统集群和数据库及存储系统。在数据库存储的数据和存储系统存储的文件层面，数据会在系统正常运行时实现两个或多个数据中心的同步，数据同步的频率依据客户的具体需求进行设定。同时，在系统容灾环境中，具有足够的数量的服务器集群，并能够在业务生产环境遭受重大灾难时接替业务生产环境的服务器集群进行工作，承接原有的用户业务流量。在灾难或重大故障发生时，京东云支持通过 DNS 切换或负载均衡切换的方式对网络进行调整，使业务流量能够顺利切换到系统容灾环境中。

应用级容灾相比于上述的数据级容灾能够承受更大的系统灾难和故障，通过冗余的计算资源承接用户的业务流量。而数据级容灾系统在服务器集群和数据库及存储系统同时遭受灾难时无法继续提供业务支撑，只能在服务器集群恢复运行后才能继续运行业务系统。

4.3.4 云产品容灾支持

4.3.4.1 云主机

京东云支持对主机的操作系统、应用程序和数据进行容灾。

操作系统容灾。不仅支持基于 X86 架构的各种物理服务器设备，也支持基于 X86 架构的云主机和虚拟机，能够实现对包括 Linux、Windows、MacOS 等多种主流操作系统的容灾。

应用程序容灾。通过旁路监听业务生产环境的数据变化，通过字节级增量数据捕捉方式将业务生产环境中变化的数据复制到系统容灾环境。通过特有的数据序列化传输技术，确保业务生产环境和系统容灾环境中数据的一致性和完整性。

数据容灾。对数据保护要求极高的客户，京东云能提供持续数据保护，并提供任意历史时间点数据恢复能力。通过字节级的数据保护技术，防止误操作、病毒、硬件故障等可能导致的数据丢失。支持在线部署容灾代理服务程序，对生产系统零影响，可保证应用运行的连续性。

4.3.4.2 数据库

数据库容灾过程中，京东云利用容灾服务实例进行生产和系统容灾环境双向通信。以极小的生产环境性能影响，在复制全量数据后通过日志同步增量数据。数据复制采用抽取-写入模式，从业务生产环境抽取数据后将数据写入到系统容灾环境，数据访问操作由数据库容灾服务代理主动发起。若数据源支持SSL，则采用 SSL 进行加密传输。也支持通过 VPN 网络进行数据复制，确保数据传输安全。

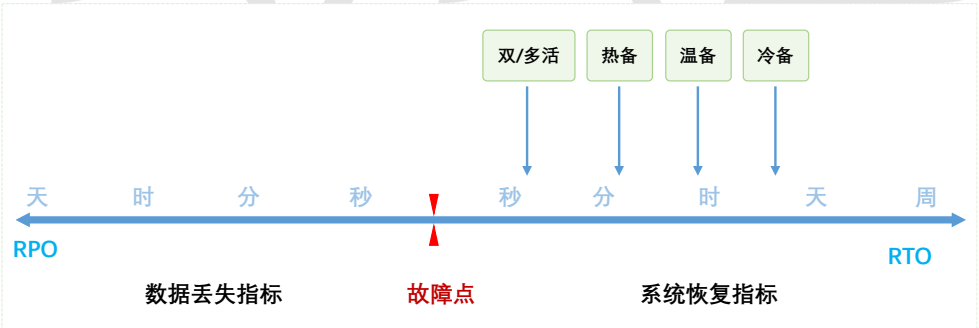
当业务生产环境的数据库发生故障时，可将业务流量转移至系统容灾环境数据库，保障业务正常运行。京东云混合云 JD Cloud Mesh 提供 SQL 级断点续传功能，无论业务生产环境、系统容灾环境还是管理端出现异常，通过断点续传功能，保障数据传输的稳定性、准确性和一致性。

4.3.5 主要指标

京东云数据库与存储产品进行系统容灾的主要指标如下表所示：

系统容灾类型	支持的方案	KPI
主机容灾	温备	RTO < 2 小时
	热备、JD Cloud Mesh 主机同步	RTO < 30 分钟
	双/多活	RTO < 2 分钟
数据库容灾	冷备	RTO < 6 小时
	温备	RTO < 1 小时
	热备、数据复制	RTO < 30 分钟
	双/多活、实时数据复制	RTO< 2 分钟

利用多种技术手段，京东云支持如下图所示的系统恢复能力：



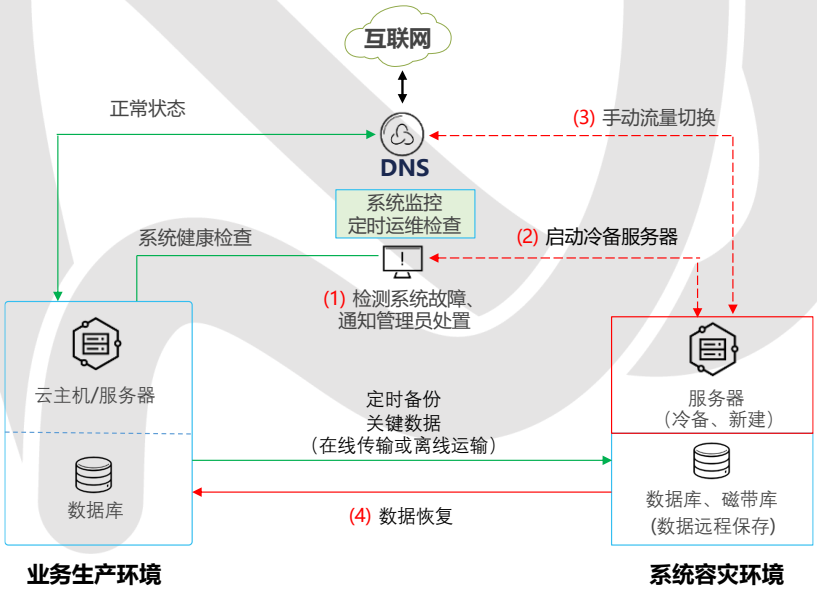
5 典型场景和行业解决方案

5.1 多级容灾解决方案

针对不同的客户需求，京东云提供多种级别系统容灾解决方案，帮助客户构建符合自身要求的系统。

5.1.1 周级容灾

针对系统故障恢复能力要求不太高的客户（一般要求 RTO≤7 天），京东云提供周级容灾解决方案，帮助客户在较少资源和人力投入的情况下实现系统的容灾保障。



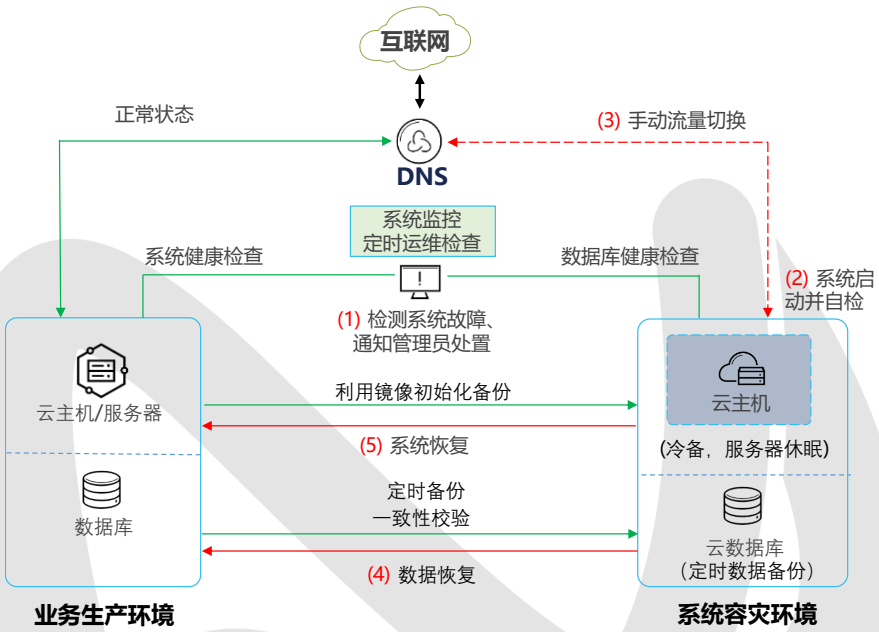
在周级容灾方案中，重点针对用户客户的关键数据进行定时备份，并且支持在同地域或跨地域建立系统容灾环境。京东云支持通过在线传输或离线运输等方式实现关键数据的离线备份。

当业务生产环境发生故障时，京东云运维系统能够快速发现系统故障并发出预警信息。在系统容灾环境中启动作为冷备的服务器资源，或者在京东云上基于原有系统设计方案重新搭建可用的业务系统，而后管理员能够将业务流量切换至系统容灾环境，并对外提供有效的服务。当原业务生产环境的资源被修复后，再将全部数据恢复至业务生产环境。

周级容灾方案能够有效保护客户关键数据不会丢失，并一定程度上确保系统在短期内能够恢复服务，不但资源占用少，还能大幅降低容灾系统的建设和维护成本。

5.1.2 天级容灾

针对系统故障恢复能力要求一般的客户（一般要求 RTO≤1 天），京东云提供天级容灾解决方案，帮助客户在一般资源和人力投入的情况下实现系统的容灾保障。



在天级系统容灾解决方案中，对客户系统中的数据进行定时备份，确保数据能够在系统容灾环境中有效保存。通过环境一致但处于长期休眠状态的冷备服务器，实现在系统容灾环境中保有能够替代业务生产环境中业务系统运行的服务器。京东云支持对业务生产环境和系统容灾环境的主机、数据库等系统进行实时的系统监控和定时的运维检查，及时发现大规模系统故障。

在业务生产环境发生大规模故障时，京东云运维系统能够第一时间检测到系统故障并对相关管理员发出预警信息。后续仅通过启动冷备服务器并进行系统自检之后，便可以将业务流量切换到系统容灾环境，使业务快速恢复运行。而后，当原有业务生产环境的资源恢复之后，在通过数据恢复和系统恢复技术使业务生产环境完全恢复。

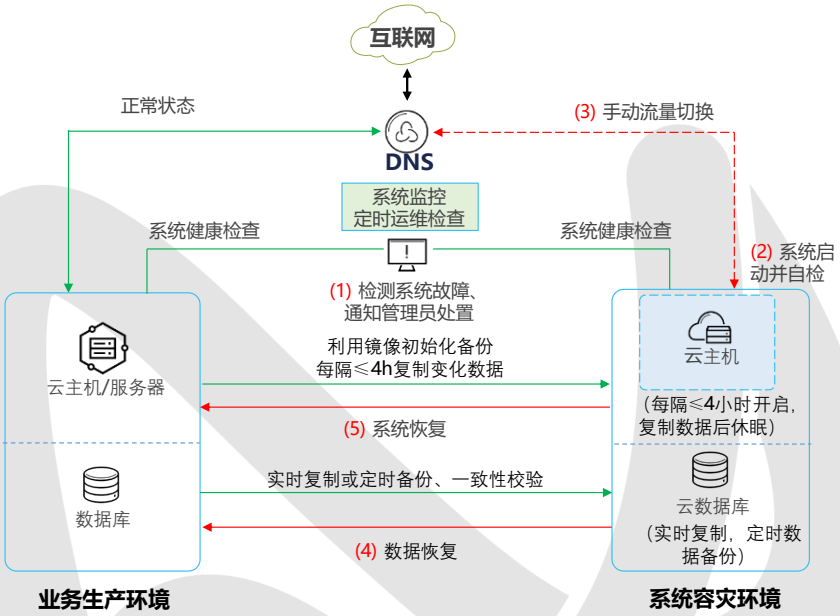
天级系统容灾方案实现了对客户业务系统的有效保护，确保客户业务系统在遭受大规模灾难时不会长期停滞，满足长期的业务良好运转。

5.1.3 小时级容灾

针对业务系统停机会带来较大损失或造成较大社会影响的系统（一般客户灾难恢复容忍度 RTO≤4 小时，RPO≤1 小时），为保障客户业务系统能够较快的恢复，京东云提供小时级容灾解决方案。

小时级系统容灾解决方案中，主要采用温备的方法对系统进行备份。在应用系统层，基于主机进行定期的状态同步。系统容灾环境中的云主机每隔一段时间（如小于 4 小时）启动运行，在完成主机的关键数据和系统状态同步之后

再进入休眠状态。在数据层，对数据库进行实时复制或定时备份，确保数据在系统容灾环境中与业务生产环境中的差异控制在一定时间范围之内。基于京东云提供的系统资源监控服务，对业务生产环境和系统容灾环境中的主机和数据库进行实时监控，能够及时发现系统故障。



当大范围系统故障发生时，监控系统会发现故障并通过多种通信渠道向系统管理员发送故障信息。此后，管理员可快速将系统容灾环境中的云主机进行启动，当完成系统自检后系统容灾环境中的云主机即可对外提供服务。此时将外部访问流量切换到系统容灾环境即可。在正常提供服务的同时，后续当原业务生产环境的资源恢复正常后，可进行数据的恢复和系统的恢复，使系统回归到正常的状态。

小时级容灾解决方案会依赖于管理员的有效操作，因此运维系统的可靠故障信息获得和及时信息传递非常关键，京东云以多年的运维保障经验积累，提供高质量运维系统，确保故障的及时发现和处置。

5.1.4 分钟级容灾

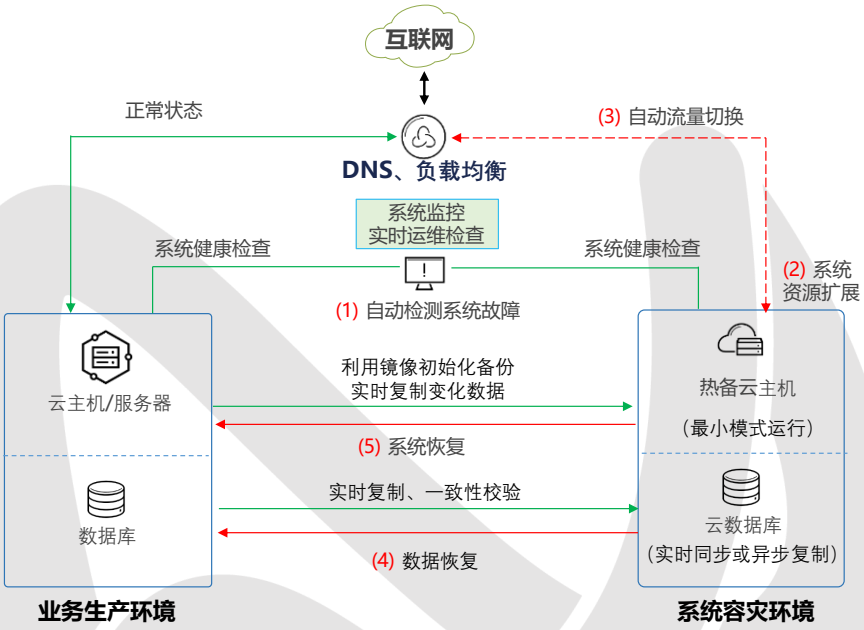
针对金融等重要行业对系统灾难恢复能力要求很高的客户，为保障快速在系统灾难中进行恢复，京东云提供分钟级系统容灾解决方案，能够实现 RTO≤30 分钟且 RPO≈0。

5.1.4.1 同城热备容灾解决方案

京东云热备容灾解决方案能够实现分钟级系统恢复能力。

京东云为客户在同城或异地提供完整的系统容灾环境，承载用于容灾的云主机和数据库资源。为降低客户建设和维护成本，可采用最小模式运行用于热

备的云主机集群。即，处于运行状态的云主机满足客户业务的最小需求，从而减少冗余资源的资源用量。利用京东云的数据复制技术，实现数据库之间的实时数据复制，保证系统容灾环境和业务生产环境中的数据一致，防止数据因故障丢失。



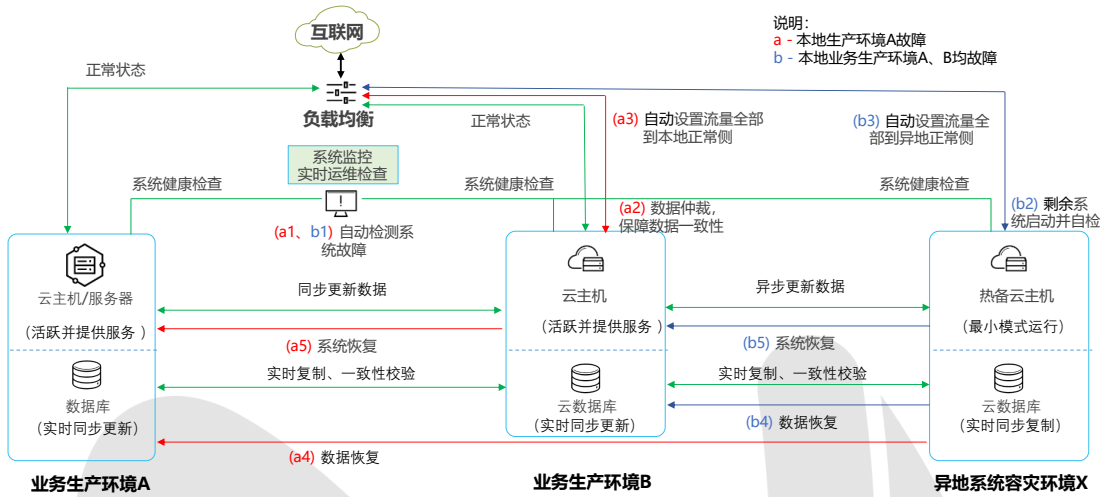
当业务生产环境因故发生大规模故障时，京东云运维监控平台能够快速反应，确保管理员能够收到及时的故障信息。在系统容灾环境，对系统中的云主机等资源进行扩展，使其能够承接当时的业务流量，而后通过网络切换将业务流量转移至系统容灾环境。整个系统故障处置过程能够在 30 分钟内完成。在业务生产环境恢复之后，也支持实现快速的数据恢复和系统恢复。

5.1.4.2 两地三中心容灾解决方案

针对大规模的业务系统，为提升业务生产环境的生产能力，同时确保系统在大规模灾难发生后能实现分钟级系统业务恢复，京东云提供基于两地三中心技术的容灾解决方案。

在两地三中心容灾解决方案中，京东云支持在同一地域内建立跨数据中心的双活系统运行环境，并在第二个地域内建立异地系统容灾环境。在同一地域内的两个数据中心中的服务器集群实现同步的数据更新，保证当任一个数据中心发生故障时另一个数据中心都能承载全部业务流量。在业务生产环境两个中心和异地系统容灾环境中的数据库利用实时复制技术实现实时同步更新，确保数据不会丢失。

当业务生产环境中的系统发生大规模故障时，通过异地系统容灾环境的支持，能够实现快速的系统业务恢复，也可以实现有效的业务生产环境恢复。



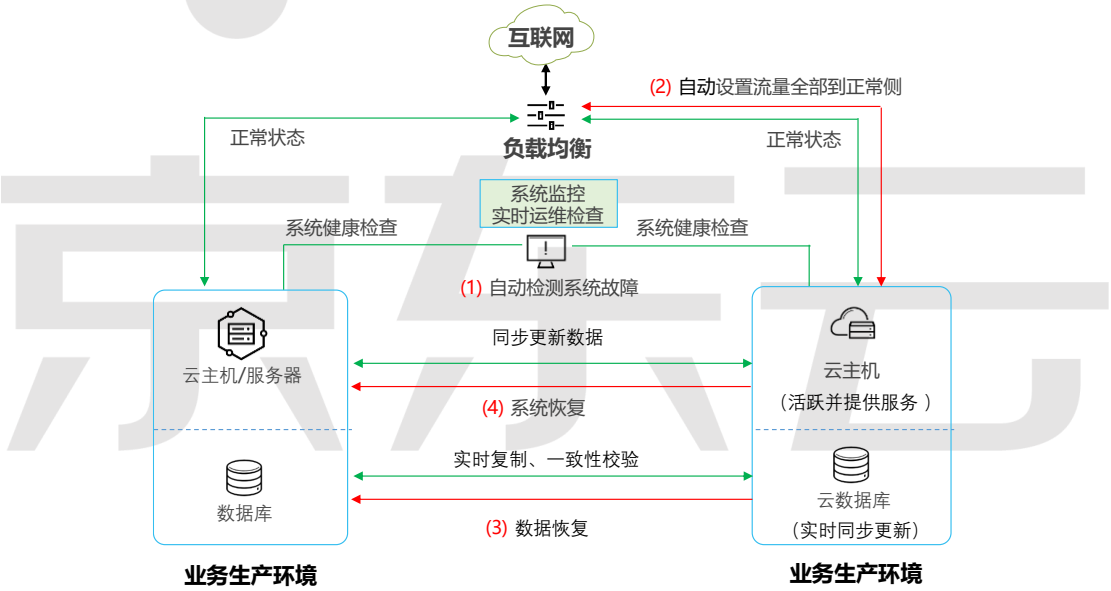
分钟级系统容灾解决方案能够为容灾需求高的客户实现更好的业务恢复能力，并有效防止数据丢失。

5.1.5 秒级容灾

针对系统灾难恢复能力要求最高的客户，京东云利用先进的负载均衡技术，提供秒级系统容灾解决方案。

5.1.5.1 同城双活容灾解决方案

同城双活容灾解决方案中，利用京东云先进的网络负载均衡技术，能够根据客户的实际业务需求实现业务流量的分配，使同一城市中的两个业务生产环境能够按指定比例均衡的处理业务流量数据。



在两个环境中的服务器中，支持实时同步需要同步的系统数据。支持数据库实时复制，并确保数据一致性，实现两个环境中的数据相同。

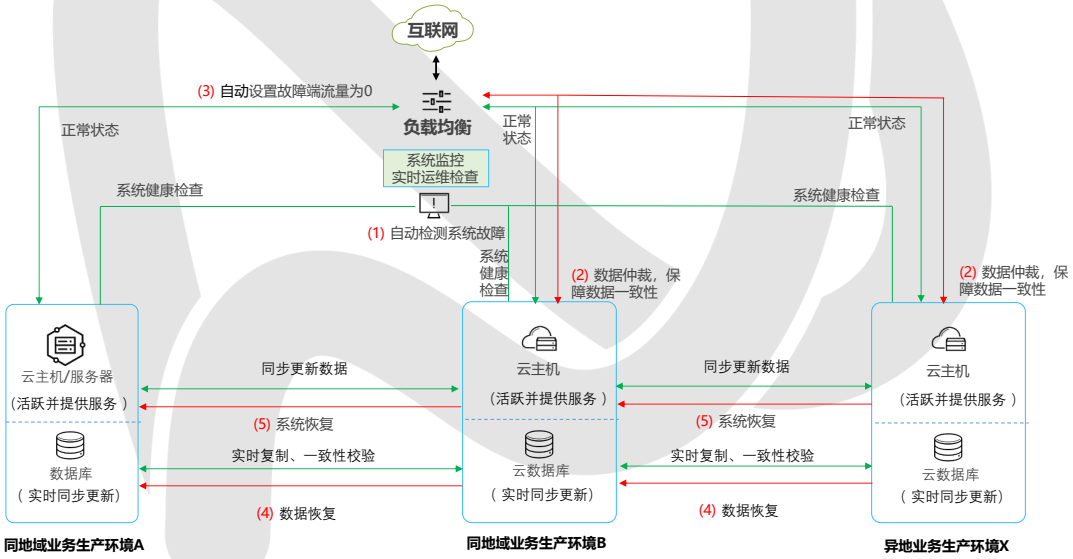
当某个业务生产环境中的系统遭遇大规模故障，网络负载均衡模块将自动

把业务流量转发至正常运行的业务生产环境，保障业务运行的连续性。在京东云公有云环境中，支持资源快速扩容，能够帮助客户支撑原有体量的客户业务请求。当故障的一侧业务生产环境恢复正常后，京东云公有云也支持快速的资源回收，确保客户业务连续性的同时，也能大幅节省成本开销。

同城双活容灾解决方案能够实现很好的业务连续性，但当城市遭遇地震等大规模灾害导致电力、通讯等基础设施全部损坏的情况下，业务生产环境也有全部无法运转的风险。

5.1.5.2 异地多活容灾解决方案

针对大规模灾害导致系统故障的风险，提供异地多活系统容灾解决方案。



在同城双活的基础上，京东云支持在异地建立支持容灾并提供业务服务的数据中心。分布在两个地域的三个或三个以上的数据中心同时对外提供业务生产服务。在这个方案中，京东云提供先进的数据同步和系统同步工具，大大降低系统建设难度，提升系统抗灾恢复能力。

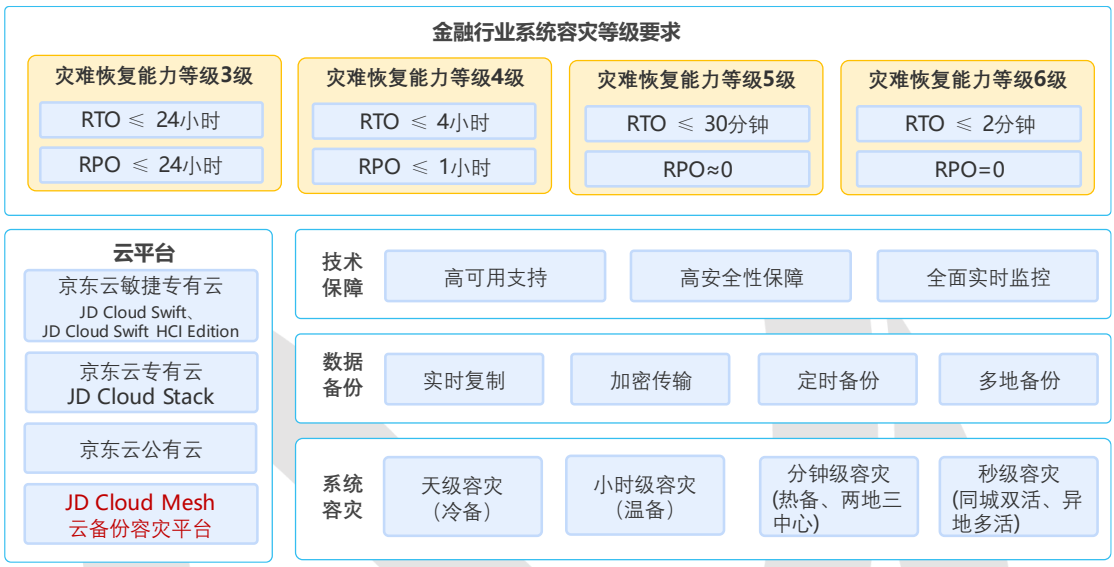
异地多活秒级系统容灾解决方案能够有效支撑对系统容灾恢复能力有最高要求的系统。

5.2 行业解决方案

5.2.1 金融行业

金融行业是关系社会民生甚至国家安全的重要行业，因此其业务系统对业务连续性要求非常高，仅能容忍非常短的系统故障恢复时间和很小系统数据因故障的损失。中国人民银行发布的《JR/T 0168-2018 云计算技术金融应用规范容灾》，明确规定了金融领域云计算平台须达到容灾能力 3 到 6 级要求。京东

云基于多年的系统建设维护技术积累，利用可靠的云平台产品，能够帮助金融客户满足金融云行业标准。



京东云提供全面实施监控服务，业务生产系统一旦遭遇灾难并发生大规模故障，能够实现及时故障信息上报，帮助管理员采取快速应急措施，保障关键金融业务的可用性。京东云支持以下多种金融级容灾方案：

- **支持容灾等级 3 级标准**

  （1）利用京东云天级容灾解决方案，实现一天之内完成灾难恢复。

  （2）支持实现 RTO≤24 小时，RPO≤24 小时，支持每年非计划服务中断时间不超过 4 天，支持系统可用性 99%以上。

- **支持容灾等级 4 级标准**

  （1）利用京东云小时级容灾解决方案，实现数小时之内完成灾难恢复。

  （2）支持 RTO≤4 小时，RPO≤1 小时，支持每年非计划服务中断时间不超过 10 小时，支持系统可用性 99.9%以上。

- **支持容灾等级 5 级标准**

  （1）利用京东云分钟级容灾解决方案，实现数分钟之内完成灾难恢复。

  （2）支持 RTO ≤30 分钟，RPO≈0， 支持每年非计划服务中断时间不超过 1 小时，支持系统可用性 99.99%以上。

- **支持容灾等级 6 级标准**

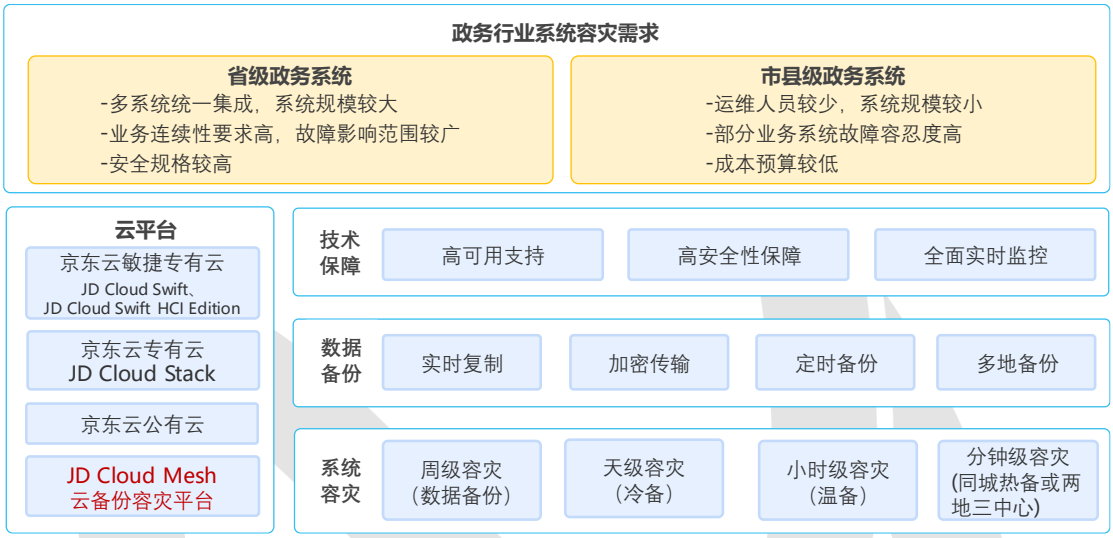
  （1）利用京东云秒级容灾解决方案，实现数秒之内完成灾难恢复。

  （2）支持 RTO≤2 分钟，RPO=0 ，支持每年非计划服务中断时间不超过 5 分钟，支持系统可用性 99.999%以上。

5.2.2 政务行业

随着智慧城市的兴起，各级政府对云计算技术越来越重视，政务系统上

云，甚至建立完善的政务云已经成为新兴的技术趋势。下面以省级和市县级政务系统为例，介绍京东云在政务行业中的系统容灾解决方案。

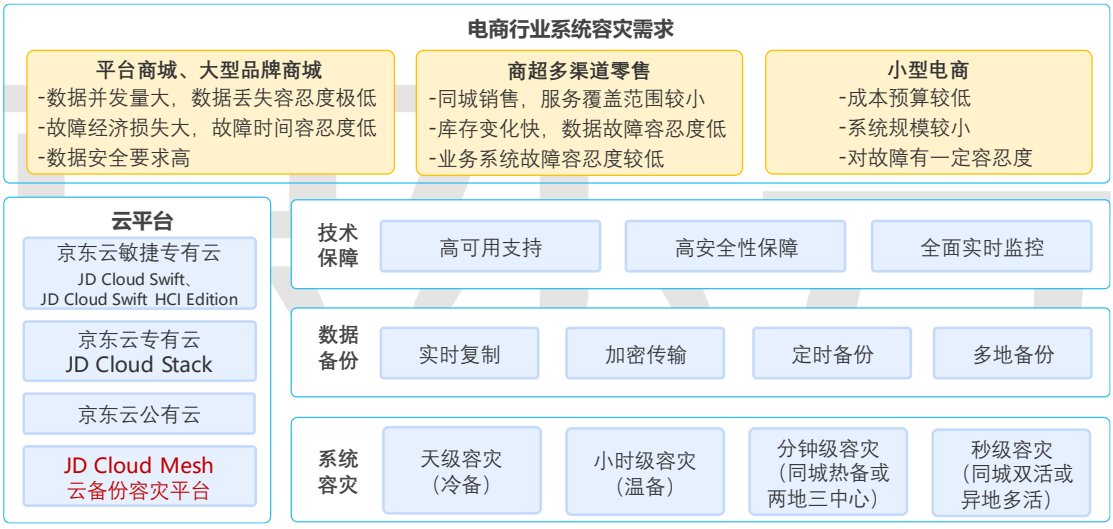


省级政务系统对业务连续性要求高，京东云提供小时级和分钟级容灾解决方案，确保关键业务系统长期稳定运行。京东云提供专有云 JD Cloud Stack 和公有云有效承载大规模省级政务系统，支撑民生建设。

市县级政务系统相对规模较小，并且运维人员相对较少，京东云支持采用公有云、专有云、或敏捷专有云提供容灾资源，并提供高质量的运维服务，并基于周或天级容灾解决方案帮助政府客户降低建设和运维成本。

5.2.3 电商行业

京东云具有强大的电商基因，因此在电商行业具有领先的云计算和系统容灾技术水平。



数据是电商的核心战略资源，数据损失将对电商的业务发展造成极为严重和深远的影响，因此京东云针对不同规模和类型的电商，在提供有效的数据容

灾保障的同时对业务连续性进行保障。

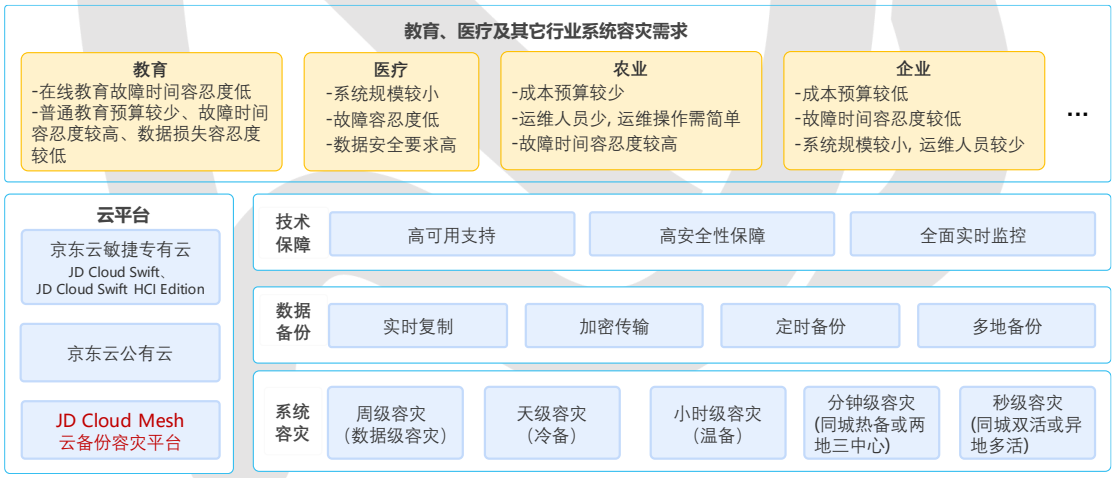
针对小型电商，京东云提供公有云、敏捷专有云等云平台资源，帮助其在实现较好的系统容灾能力的同时，有效降低系统建设和运维成本。

针对商超零售客户，京东云在提供完整的电商解决方案的同时，基于公有云和专有云提供强大的计算、存储、网络资源，同时利用架构设计优势，确保在灾难情况下数据损失小，系统恢复快。

针对平台商城和大型品牌商城等大型电商客户，京东云在技术和服务方面提供全方位支撑，不但能保证业务系统的连续性，还通过提供整个生态系统的支持帮助客户不断实现业务发展和突破。

5.2.4 教育、医疗及其它行业

京东云对各个行业均能提供有针对性的有效系统容灾解决方案。



随着互联网技术的发展，教育云发展极为迅速，生发出众多细分行业，最有代表性的为传统普通教育云与在线教育云。京东云针对各个细分行业，提供有针对性的系统容灾解决方案，确保客户的数据得到有效的保护，保障业务连续性满足客户需求预期。

京东云还针对医疗、农业、广大企业等各行各业的客户，基于行业和客户的具体系统容灾需求，提供专业的系统架构设计和实施方案，有效提升客户业务系统的容灾能力。

6 总结

数据备份和系统容灾是保障客户业务长期有效运行的关键技术。基于京东云多年在数据备份和系统容灾技术领域的积累和探索，深入介绍了京东云的技术方法和技术能力，向关心系统容灾能力的企业领导者和核心技术人员分享了京东云的多级容灾解决方案，帮助客户解决各个场景下的数据备份和数据容灾技术问题。

并基于京东云对行业的理解和技术积淀，分享了不同行业中的典型解决方案。为客户基于京东云轻松构建安全、可靠的业务系统提供有价值的技术参考。

7 引用

[1] 《JR/T 0168-2018 云计算技术金融应用规范 容灾》，中国人民银行

[2] 《重要信息系统灾难恢复指南》，国务院信息化工作办公室

[3] 《GB/T 20988-2007 信息安全技术 信息系统灾难恢复规范》，国家质量监督检验检疫总局